MICHIGAN

OFFICE OF THE AUDITOR GENERAL

AUDIT REPORT

PERFORMANCE AUDIT
OF

NETWORK APPLICATION SERVER CONTROLS

DEPARTMENT OF INFORMATION TECHNOLOGY

October 2006

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

084-0555-05

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

– Article IV, Section 53 of the Michigan Constitution

Audit report information can be accessed at:
http://audgen.michigan.gov

Michigan

Office of the Auditor General

REPORT SUMMARY

Performance Audit

Network Application Server Controls

Department of Information Technology

Report Number:
084-0555-05

Released:
October 2006

The Department of Information Technology (DIT) is responsible for achieving a unified and more cost-effective approach for managing information technology. The State has approximately 600 network application servers that are primarily configured, managed, and secured by DIT's Technical Services Division with the assistance of DIT's Office of Enterprise Security. Management and security controls over network application servers directly affect the confidentiality, integrity, and availability of data on the State's information network.

Audit Objective:
To assess the effectiveness of DIT's efforts to ensure that network application servers have been properly configured in accordance with standards and best practices.

Audit Conclusion:
DIT's efforts to ensure that network application servers have been properly configured in accordance with standards and best practices were not effective.

Material Conditions:
DIT did not control or provide oversight of all the State's network application server resources as required by Executive Order No. 2001-3. As a result, DIT cannot ensure that those network application servers administered outside of the Technical Services Division are configured, managed, and secured based on DIT's policies, standards, procedures, or industry best practices. (Finding 1)

DIT and its customer agencies had not established a complete list of network application servers that were critical to State operations. As a result, DIT and its customer agencies cannot focus their limited information technology resources on securing the State's most critical information systems. (Finding 2)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT's policies and procedures to ensure the security of network application servers.

Audit Conclusion:
DIT's policies and procedures to ensure the security of network application servers were not effective.

Material Condition:
DIT did not establish, implement, update, communicate, and train staff in comprehensive technical policies, standards, and procedures that complement the State's technology architecture plan to create an enterprise-wide system and comply with Control Objectives for Information and Related Technology (COBIT) standards. As a result, DIT cannot ensure that it was practicing

due diligence in its management and security of the State's network application servers. (Finding 3)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Audit Objective:
To assess the effectiveness of DIT's management plans to support the system administration function.

Audit Conclusion:
DIT's management plans to support the system administration function were not effective.

Material Condition:
DIT had not defined its future operating environment or developed an implementation plan to achieve it. Without a defined future operating environment and implementation plan, DIT cannot ensure that its current initiatives address the challenges of establishing an effective and efficient system administration function to support the State's network application servers. (Finding 4)

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

Agency Response:
Our audit report contains 4 findings and 4 corresponding recommendations. DIT's preliminary response indicates that it agrees with all of the recommendations and will comply with them.

~ ~ ~ ~ ~ ~ ~ ~ ~ ~

A copy of the full report can be obtained by calling 517.334.8050 or by visiting our Web site at: http://audgen.michigan.gov

Michigan Office of the Auditor General
201 N. Washington Square
Lansing, Michigan 48913

Thomas H. McTavish, C.P.A.
Auditor General

Scott M. Strong, C.P.A., C.I.A.
Deputy Auditor General

STATE OF MICHIGAN
OFFICE OF THE AUDITOR GENERAL
201 N. WASHINGTON SQUARE
LANSING, MICHIGAN 48913
(517) 334-8050
FAX (517) 334-8079

THOMAS H. MCTAVISH, C.P.A.
AUDITOR GENERAL

October 31, 2006

Ms. Teresa M. Takai, Director
Department of Information Technology
George W. Romney Building
Lansing, Michigan

Dear Ms. Takai:

This is our report on the performance audit of Network Application Server Controls, Department of Information Technology.

This report contains our report summary; description of agency; audit objectives, scope, and methodology and agency responses; comments, findings, recommendations, and agency preliminary responses; and a glossary of acronyms and terms.

Our comments, findings, and recommendations are organized by audit objective. The agency preliminary responses were taken from the agency's responses subsequent to our audit fieldwork. The *Michigan Compiled Laws* and administrative procedures require that the audited agency develop a formal response within 60 days after release of the audit report.

We appreciate the courtesy and cooperation extended to us during this audit.

Sincerely,

Thomas H. McTavish, C.P.A.
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

NETWORK APPLICATION SERVER CONTROLS
DEPARTMENT OF INFORMATION TECHNOLOGY

Description of Agency

The Department of Information Technology (DIT) was created in October 2001 by Executive Order No. 2001-3 to achieve a unified and more cost-effective approach for managing information technology* (IT) among all executive branch agencies.

DIT's Technical Services Division is responsible for configuring and managing approximately 600 network application servers*. Management controls* and security controls over network application servers directly affect the confidentiality*, integrity*, and availability* of data on the State's information network. DIT's Technical Services Division and Office of Enterprise Security (OES) share responsibility for securing the State's network application servers.

Technical Services Division

Prior to the formation of DIT in 2001, each State department maintained its own network application servers. The Department of Management and Budget (DMB) provided agencies with overall network application server security guidance. Departments were responsible for establishing policies and procedures to fit their specific information systems' environment. When DIT was established, each State department's system administration* function was transferred to DIT. The responsibility for providing server security guidance was also transferred from DMB to DIT.

DIT realigned in March 2004 and placed system administration functions in a consolidated area called the Technical Services Division. The network application servers within the Technical Services Division are administered by system administrators in the IT programmer analyst and IT specialist classifications and by several contractors. These system administrators are organized into 12 teams that operate independently from each other. The majority of these teams remained grouped according to the original agency that they came from when DIT was created and still service the original agency's servers following the operating practices that were in place at the original agency.

* *See glossary at end of report for definition.*

Office of Enterprise Security (OES)

OES is responsible for identifying, managing, and mitigating security risks* and vulnerabilities* within the State of Michigan government computing, communication, and technology resources. OES is also responsible for disaster recovery planning, risk management, security awareness and training, assistance to State agencies with their security issues, and enforcement oversight of State security policies and procedures intended to maintain suitable enterprise-wide security.

Standards and Policy Review Board (SPRB)

SPRB was created in June 2005 by the DIT executive team. SPRB formalizes the process of creating and updating technical standards and policies. SPRB has the responsibility and authority to oversee the creation, review, and approval of technology standards and policies. Its function is to set standards for IT acquisition and technical policies for entities served or supported by DIT.

SPRB has the following objectives:

1. Review and approve IT standards, policies, architectures, and guidelines.

2. Oversee standards development teams.

3. Ensure that technology standards are aligned with the enterprise strategic plans.

4. Ensure that technology standards result in effective, realistic, and reasonable implementations.

SPRB is a cross-functional board composed of representatives from various areas of DIT, including the Bureau of Strategic Policy, Field Services Division, Data Center Services Division, Technical Services Division, Telecommunications and Network Management Division, OES, and Agency Services Division.

* *See glossary at end of report for definition.*

Audit Objectives, Scope, and Methodology and Agency Responses

Audit Objectives

Our performance audit* of Network Application Server Controls, Department of Information Technology (DIT), had the following objectives:

1. To assess the effectiveness* of DIT's efforts to ensure that network application servers have been properly configured in accordance with standards and best practices.

2. To assess the effectiveness of DIT's policies and procedures to ensure the security of network application servers.

3. To assess the effectiveness of DIT's management plans to support the system administration function.

Audit Scope

Our audit scope was to examine the information processing and other records related to network application server controls. Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States and, accordingly, included such tests of the records and such other auditing procedures as we considered necessary in the circumstances.

Audit Methodology

Our audit procedures, performed from May 2005 through January 2006, included examination of DIT's network application server processes and other records primarily for the period October 1, 2004 through November 30, 2005. The criteria used in the audit included control guidelines outlined in the Control Objectives for Information and Related Technology* (COBIT), issued by the Information Systems Audit and Control Foundation (ISACF) in July 2000, and guidelines issued by the National Institute of Standards and Technology (NIST), as well as other information security best practices.

* *See glossary at end of report for definition.*

To accomplish our audit objectives, our audit methodology included the following phases:

1. Preliminary Review and Evaluation Phase

   We conducted a preliminary review of DIT's efforts to ensure the security of the State's network application servers. We reviewed and obtained an understanding of DIT's policies, standards, and procedures for network application server administration. We obtained an understanding of the organizational controls for the system administration function. We used the results of our review to determine the extent of our detailed analysis and testing.

2. Detailed Analysis and Testing Phase

   We performed an assessment of DIT's efforts to ensure that the network application servers are configured in accordance with best practices and an assessment of the effectiveness of DIT's policies and procedures to ensure the security of network application servers. We also assessed the effectiveness of DIT's management plans to support the system administration function:

   a. Effectiveness of server configurations:

      (1) We reviewed DIT's assessments of vulnerability scans conducted on publicly accessed network application servers.

      (2) We evaluated DIT's process for identifying critical network application servers.

   b. Effectiveness of policies and procedures:

      (1) We reviewed and evaluated policies and procedures regarding system administration, policies for assigning responsibility and authority for server security management, and the process for communicating policies and procedures to system administrators.

      (2) We interviewed DIT management to determine how system administration policies and procedures were complied with and enforced.

(3) We reviewed and analyzed position descriptions and individual development plans (IDPs) of various levels of DIT management to determine responsibilities for the creation and maintenance of policies and procedures.

c. Effectiveness of management plans:

(1) We interviewed DIT management to understand the objectives for the operating environment that would support the system administration function.

(2) We requested and reviewed all management plans for the system administration function.

(3) We evaluated the position descriptions for system administrators to determine if they were documented and up to date.

(4) We reviewed the IDPs for system administrators to assess whether they were being used as an effective tool to identify training needs.

3. Evaluation and Reporting Phase

We evaluated and reported on the results of the detailed analysis and testing phase.

Agency Responses

Our audit report contains 4 findings and 4 corresponding recommendations. DIT's preliminary response indicates that it agrees with all of the recommendations and will comply with them.

The agency preliminary response that follows each recommendation in our report was taken from the agency's written comments and oral discussion subsequent to our audit fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and Department of Management and Budget Administrative Guide procedure 1280.02 require DIT to develop a formal response to our audit findings and recommendations within 60 days after release of the audit report.

COMMENTS, FINDINGS, RECOMMENDATIONS, AND AGENCY PRELIMINARY RESPONSES

EFFECTIVENESS OF NETWORK APPLICATION SERVER CONFIGURATION

COMMENT

Audit Objective: To assess the effectiveness of the Department of Information Technology's (DIT's) efforts to ensure that network application servers have been properly configured in accordance with standards and best practices.

Conclusion: DIT's efforts to ensure that network application servers have been properly configured in accordance with standards and best practices were not effective. Our assessment disclosed two material conditions*. DIT did not control or provide oversight of all the State's network application server resources as required by Executive Order No. 2001-3 (Finding 1). Also, DIT and its customer agencies had not established a complete list of network application servers that were critical to State operations (Finding 2).

This conclusion is also supported by audit work performed for the other two audit objectives in this report. DIT's ineffective policies, procedures, and management controls prevent it from properly configuring servers. In addition, the results of vulnerability scans of network application servers conducted by DIT revealed a significant number of high-risk vulnerabilities that, if compromised, could adversely impact the State's information systems and its ability to provide mission critical services to the public. DIT informed us that it conducted vulnerability scans in May through June 2005 and then began remediation efforts. In August 2005, remediation efforts were in process. DIT assigned responsibility, developed solutions, and initiated efforts to remediate the vulnerabilities identified in its scans. In addition, DIT acknowledged that an enterprise level approach to network application server support is needed to improve service delivery and information security.

FINDING

1. Network Application Servers Outside of Technical Services Division's Control

   DIT did not control or provide oversight of all the State's network application server resources as required by Executive Order No. 2001-3. As a result, DIT cannot ensure that those network application servers administered outside of the

* *See glossary at end of report for definition.*

Technical Services Division are configured, managed, and secured based on DIT's policies, standards, procedures, or industry best practices.

Executive Order No. 2001-3 gave DIT the authority and responsibility for all information technology (IT) resources of the executive branch, including network application server resources. The Executive Order required DIT to adopt industry best practices and provide efficient and consistent service delivery to State agencies.

Our review disclosed the following areas in which DIT did not provide effective control and oversight:

a. DIT did not ensure that all network application servers were transferred and subjected to DIT's control nor did DIT establish written agreements with other State agencies to whom DIT had delegated responsibility for server security and administration. In addition, DIT did not monitor or ensure that State agencies administered and secured these servers in a manner consistent with State standards. DIT should use its authority from the Executive Order and either take direct control of all State network application server resources or establish written agreements and monitor State agencies to ensure compliance with State security standards.

b. DIT did not ensure that all DIT system administrators reported to their appropriate managers according to DIT organizational charts. We noted, based on payroll records, that some DIT system administrators reported to the State agencies they support rather than to a DIT Technical Services Division manager. Technical Services Division managers should be directly responsible for all DIT system administrators to ensure adequate oversight.

c. DIT allowed employees in its Agency Services Division to function as system administrators for some network application servers. System administration is not the role and responsibility of the Agency Services Division. DIT should transfer these system administration functions and resources to its Technical Services Division. Centralized administration of network application servers will improve service delivery and reduce administrative costs.

RECOMMENDATION

We recommend that DIT control or provide oversight of all the State's network application server resources as required by Executive Order No. 2001-3.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT will control and monitor or establish written agreements and provide oversight to all of the State's network application server resources to ensure that all network application servers are configured, managed, and secured based on DIT's policies, standards, procedures, or industry best practices. DIT Technical Services Division managers will be directly responsible for DIT network application system administrators to ensure adequate oversight. DIT will transfer system administration functions and resources managed by the Agency Services Division to the Technical Services Division. DIT will work to achieve full compliance by December 31, 2007.

FINDING

2. Identification of Critical Network Application Servers

DIT and its customer agencies had not established a complete list of network application servers that were critical to State operations. As a result, DIT and its customer agencies cannot focus their limited IT resources on securing the State's most critical information systems.

DIT used several methods and criteria in its attempts to inventory and identify critical servers and information resources. However, the criteria that DIT used narrowly focused on business continuity and did not address the important security objectives of confidentiality and integrity of information and information systems.

The federal government's Computer Security Division, National Institute of Standards and Technology (NIST), provides generally accepted guidance to assess the criticality of information and information systems. Federal Information Processing Standard 199 establishes security categories for information and information systems based on the potential impact on an organization. Security categories are to be used in conjunction with vulnerability and threat* information in assessing the security risk to an organization.

* *See glossary at end of report for definition.*

RECOMMENDATION

We recommend that DIT and its customer agencies establish a complete list of network application servers that are critical to State operations.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT will continue its work with the other agencies to establish a complete list of network application servers that are critical to State operations. DIT will expand its criteria requirements for critical applications to include the security and internal control* objectives of confidentiality, integrity, and availability of information and information systems. DIT informed us that a complete inventory of network application servers that are critical to State operations will be available by March 2007.

EFFECTIVENESS OF POLICIES AND PROCEDURES

COMMENT

Background: In February 2005, DIT formally adopted Control Objectives for Information and Related Technology (COBIT) to assist management in ensuring that a security and internal control framework was in place for the State of Michigan's IT environment.

Audit Objective: To assess the effectiveness of DIT's policies and procedures to ensure the security of network application servers.

Conclusion: DIT's policies and procedures to ensure the security of network application servers were not effective. Our assessment disclosed one material condition. DIT did not establish, implement, update, communicate, and train staff in comprehensive technical policies, standards, and procedures that complement the State's technology architecture plan to create an enterprise-wide system and comply with COBIT standards (Finding 3).

* *See glossary at end of report for definition.*

FINDING

3. Technical Policies

DIT did not establish, implement, update, communicate, and train staff in comprehensive technical policies, standards, and procedures that complement the State's technology architecture plan to create an enterprise-wide system and comply with COBIT standards. As a result, DIT cannot ensure that it was practicing due diligence* in its management and security of the State's network application servers.

Section 18.1485(3) of the *Michigan Compiled Laws* (Act 431, P.A. 1984) requires each department's director to document, to communicate, and to ensure compliance with managerial policies.

Our review of DIT's operating practices and interviews with DIT Technical Services Division management disclosed:

a. Although DIT formally adopted COBIT, DIT had not established and implemented policies recommended by COBIT, NIST publications, the International Standards Organization (ISO) 17799*, and the State's *Secure Michigan Initiative**. As a result, management did not provide system administration policies in areas such as policy communication, defined roles and responsibilities for system administrators, server security certification* and accreditation*, server reaccreditation, security training and education, and segregation of duties*.

Without providing guidance to system administrators, DIT cannot ensure that critical security controls are in place and security is effective.

COBIT states that management's intentions should be communicated through the use of policies and procedures. In addition, COBIT states that an organization cannot achieve a positive control environment if it has not defined, documented, and communicated its policies or procedures.

* *See glossary at end of report for definition.*

b. DIT did not update existing technical server security and administration policies to ensure that the policies complement the State's technology architecture plan and comply with COBIT.

Outdated policies do not effectively communicate management's expectations for network application server security and prevent DIT from achieving a unified approach to system administration.

COBIT states that policies should be regularly re-evaluated for adequacy and appropriateness and amended as necessary.

c. DIT did not ensure that server teams were aware of and following technical policies, standards, or procedures. As a result, DIT cannot ensure consistent, efficient, and effective network application server security and administration.

For example, DIT's server security policy 1350.11 represents the single most significant guidance that, if followed, would reduce the security risk to the State's network application servers and information systems. However, DIT management did not distribute server security policies to system administrators primarily responsible for server security. If DIT had enforced this policy, server vulnerabilities and security risks would have been reduced.

d. DIT did not train its Technical Services Division staff on COBIT standards.

DIT formally adopted COBIT to assist management in ensuring that a security and internal control framework is in place for the State's IT environment. COBIT control objectives and practices are designed to help ensure the development of effective policies and procedures by providing a framework of generally accepted practices for managing and controlling information and IT resources. Without staff training in COBIT, DIT cannot ensure that the Technical Services Division includes COBIT's IT control standards and recommendations in the development of policies and procedures.

DIT policy 100.16 states that DIT employees should integrate COBIT into their business practices, policies, and procedures.

e. DIT did not conduct periodic technical security training for system administrators.

   Without periodic training in general security policies and procedures and platform* specific security controls, DIT cannot ensure that system administrators are sufficiently knowledgeable to adequately secure the servers they manage. In addition, until employees are sufficiently trained and knowledgeable in a policy, standard, or procedure, DIT cannot enforce compliance.

To facilitate its efforts to comply with COBIT standards, DIT should seek guidance from IT standards groups, such as NIST and ISO, that have established the foundation for organizations to develop and implement technical policies and procedures. Specifically, the NIST 800 series of special publications offers detailed guidance in technical policies and procedures.

RECOMMENDATION

We recommend that DIT establish, implement, update, communicate, and train staff in comprehensive technical policies, standards, and procedures that complement the State's technology architecture plan to create an enterprise-wide system and comply with COBIT standards.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT will continue to work to establish, implement, update, communicate, and train staff in comprehensive technical policies, standards, and procedures that comply with COBIT standards. DIT Enterprise Architecture (in conjunction with the Office of Enterprise Security and the Technical Services Division) will update existing technical policies that align with DIT's adoption of the *Secure Michigan Initiative* and COBIT by June 30, 2007. DIT informed us that training is an ongoing commitment and COBIT training will be held for the Technical Services Division by June 30, 2007. DIT will work to achieve full compliance by December 31, 2007.

* *See glossary at end of report for definition.*

EFFECTIVENESS OF MANAGEMENT PLANS

COMMENT

Background: One of the goals from Michigan's 1999 IT Strategic Plan was to acquire, retain, and maintain a highly qualified IT work force. The State of Michigan IT Assessment and Benchmarking Project Assessment Report, issued by Deloitte Consulting in February 2000, stated that the availability of qualified State IT resources could be enhanced. For example, the report indicated that, because of an aging work force, staff may not be sufficiently skilled for meeting the demands of newer technologies and directions of the State departments. The report also indicated that, despite the aging work force, there was little effort by the State to train and educate State employees who showed interest in and the capacity for careers as IT professionals. It also stated that the IT functions needed a clear governance structure defining organizational behavior in terms of an accountability framework for roles and responsibilities and service delivery.

At the time that the 1999 IT Strategic Plan and the Deloitte Consulting report were issued, each State department maintained its own IT infrastructure and employed a team of system administrators. In 2001, Executive Order No. 2001-03 was implemented, which created DIT for the purpose of achieving an enterprise-wide management structure of the State's information systems. After the creation of DIT and the transfer of system administrators to DIT in 2001, the system administrators continued to operate in agency specific teams independent of one another.

The purpose of our review of this area was to assess the effectiveness of DIT's management plans to create, implement, and maintain an enterprise-wide system administration function. Many of the organizational issues identified in the 1999 IT Strategic Plan and the Deloitte Consulting report still exist.

Audit Objective: To assess the effectiveness of DIT's management plans to support the system administration function.

Conclusion: DIT's management plans to support the system administration function were not effective. Our assessment disclosed one material condition. DIT had not defined its future operating environment or developed an implementation plan to achieve it (Finding 4).

FINDING

4. Management Plans

DIT had not defined its future operating environment or developed an implementation plan to achieve it. Without a defined future operating environment and implementation plan, DIT cannot ensure that its current initiatives address the challenges of establishing an effective and efficient system administration function to support the State's network application servers.

The Government Accountability Office (GAO) established guidance for developing a future operating environment and implementation plan. The GAO guidance states that there should be a program that will provide for the development of architectural descriptions of how the organization currently operates, how it intends to operate in the future, and how it will transition from the current operating environment to the future environment.

The Technical Services Division is working on several projects, referred to as the Michigan/1 Initiative, that address the technical architecture. As part of this Initiative, DIT is physically centralizing and consolidating its servers. However, the Michigan/1 Initiative has not addressed the organizational challenges for system administration.

Our review identified the following organizational challenges that DIT should address while defining its future operating environment and implementation plan:

a. DIT had not defined the detailed technical and security competencies* to perform the system administration function. DIT had identified extensive behavioral competencies* needed to perform the system administration function. Identifying the detailed technical and security competencies would assist in defining job classifications and positions and in guiding training efforts.

b. DIT had not defined the job classification structure that would support its future operating environment. The current IT job classifications were established prior to the formation of DIT. These job classifications do not define

* *See glossary at end of report for definition.*

the specific duties and responsibilities or the required knowledge, skills, and abilities needed to support the server administration function. COBIT recommends that skill requirements to meet short- and long-range IT needs of the organization be defined. Therefore, DIT should continue to work with the Department of Civil Service to establish specific job classifications that will ensure proper configuration, administration, and security of network application servers.

c. DIT did not have documented, complete, up-to-date, and accurate position descriptions for all system administrators. Further, the Technical Services Division did not identify the positions needed to operate in its future operating environment and how the positions will be transitioned. The position descriptions for many of the system administrators were not formally documented, had not been updated to reflect changes since DIT was established, or contained incompatible duties. Communicating roles and responsibilities and identifying the positions for the future would help ensure that system administrators perform only those job functions for which they are qualified and that incompatible duties are properly segregated.

d. DIT did not complete a gap analysis between the skills needed and the skills currently available for the system administration function. A gap analysis would help the Technical Services Division to more effectively train its system administrators by focusing limited training resources on specific skill deficiencies.

e. DIT did not prepare complete individual development plans (IDPs) for system administrators. DIT developed a process to assist managers in identifying the training needs of system administrators; however, because of limited training funds, managers did not include all training needs in IDPs. DIT could more accurately assess its training needs and budget if managers included all training needs in IDPs.

f. DIT did not complete the technical training curriculum for the server support job role. The training curriculum would help ensure that DIT focuses training efforts on the technical and security competencies needed in the future operating environment.

RECOMMENDATION

We recommend DIT define its future operating environment and develop an implementation plan to achieve it.

AGENCY PRELIMINARY RESPONSE

DIT agrees and will comply with the recommendation. DIT will continue to define its operating environment and implement action plans that ensure current initiatives address the challenges of establishing an effective and efficient system administration function to support the State's network application servers. DIT informed us that it has launched the Technical Services Optimization project which, in May 2006, established senior standards and the core classification (including job duties and position descriptions) for the Technical Services Division. In addition, DIT informed us that, during the past nine months, it has completed 64% of all Technical Services Division IDPs and that the remaining 36% will be completed by March 2007. DIT will partner with the Department of Civil Service to further refine the current IT classification and compensation system. DIT will work to achieve full compliance by December 31, 2007.

GLOSSARY

accreditation	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
availability	Timely and reliable access to and use of data.
behavioral competencies	Observable, measurable patterns of qualities that individuals need to perform their job function, such as adaptability, communication, and leadership.
certification	A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
confidentiality	The assurance that data is not disclosed to unauthorized individuals or processes.
Control Objectives for Information and Related Technology (COBIT)	A framework, control objectives, and audit guidelines developed by the Information Systems Audit and Control Foundation (ISACF) as a generally applicable and accepted standard for good practices for controls over information technology.
DIT	Department of Information Technology.
DMB	Department of Management and Budget.

due diligence	The degree of care that a reasonable person might be expected to exercise under the same circumstances.
effectiveness	Program success in achieving mission and goals.
GAO	Government Accountability Office.
IDP	individual development plan.
information technology (IT)	Any equipment or interconnected system that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It commonly includes hardware, software, procedures, services, and related resources.
integrity	The accuracy, completeness, and timeliness of data in an information system.
internal control	The organization, policies, and procedures adopted by agency management and other personnel to provide reasonable assurance that operations, including the use of agency resources, are effective and efficient; financial reporting and other reports for internal and external use are reliable; and laws and regulations are followed. Internal control also includes the safeguarding of agency assets against unauthorized acquisition, use, or disposition.
International Standards Organization (ISO) 17799	A detailed security standard published by ISO. ISO17799 is organized into 10 major sections.
management controls	The organization, policies, and procedures used to provide reasonable assurance that (1) programs achieve their intended result, (2) resources are used consistent with the organization's mission, (3) programs and resources are

	protected from waste, fraud, and mismanagement, (4) laws and regulations are followed, and (5) reliable and timely information is obtained, maintained, reported, and used for decision-making.
material condition	A reportable condition that could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program.
network application server	A computer dedicated to running certain software applications, such as Web, database, payroll, personnel, accounting, and licensing, in a computer network.
NIST	National Institute of Standards and Technology.
OES	Office of Enterprise Security.
performance audit	An economy and efficiency audit or a program audit that is designed to provide an independent assessment of the performance of a governmental entity, program, activity, or function to improve public accountability and to facilitate decision making by parties responsible for overseeing or initiating corrective action.
platform	The type of operating system or computer being used.
reportable condition	A matter that, in the auditor's judgment, represents either an opportunity for improvement or a significant deficiency in management's ability to operate a program in an effective and efficient manner.
Secure Michigan Initiative	A self-assessment report conducted by DIT in 2002 that identified the security risks, threats, and vulnerabilities of the State's entire computer system and provided security

	recommendations to minimize the identified risks, threats, and vulnerabilities.
security risk	The probability that a particular security threat will exploit a system vulnerability.
segregation of duties	Separation of the management or execution of certain duties or areas of responsibility in order to prevent and reduce opportunities for unauthorized modification or misuse of data or service.
SPRB	Standards and Policy Review Board.
system administration	The process of installing, configuring, and maintaining the networks, computers, and system security in an organization.
technical and security competencies	The professional skills and knowledge that individuals need to perform their specific job function. System administrator technical and security competencies could include performance tuning tools and techniques, configuration management, and contingency planning.
threat	An activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank


STATE OF MICHIGAN
OFFICE of the AUDITOR GENERAL